



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/922,041	08/03/2001	Larry H. Gass	ITL.0506US (P10475)	7270
21906	7590	11/16/2007		
TROP PRUNER & HU, PC 1616 S. VOSS ROAD, SUITE 750 HOUSTON, TX 77057-2631			EXAMINER NGUYEN, MINH DIEU T	
			ART UNIT 2137	PAPER NUMBER
			MAIL DATE 11/16/2007	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

## Office Action Summary

Application No.

09/922,041

Applicant(s)

GASS ET AL.

Examiner

Minh Dieu Nguyen

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 30 August 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1, 3-7, 27, 29 and 32-42 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1, 3-7, 27, 29 and 32-42 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☐ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- ☐ Notice of Informal Patent Application
- ☐ Other: \_\_\_\_\_

## **DETAILED ACTION**

### ***Response to Amendment***

1. This office action is in response to the communication dated August 30, 2007 with the amendments to claims 1, 27, 32-33 and 39-42.
2. Claims 1, 3-7, 27, 29, and 32-42 are pending.

### ***Response to Arguments***

3. Applicant's arguments filed August 30, 2007 have been fully considered but they are not persuasive. Applicant argues that the amended limitation has two portions of the same reprogrammable semiconductor memory. In contrast, in Hind, two separate memories are utilized, only one of which is reprogrammable. The Examiner respectfully disagrees, Hind discloses a single memory array may be utilized to provide the programmable memory and the read only memory (Hind: col. 9, lines 29-32), as such two portions of a firmware code (i.e. upgradable and non-upgradable) are in the same reprogrammable memory.

Regarding the rejection of claims 1, 3, 5-7, 27 and 29, the Applicant argues that the prior arts do not teach retrieving a second public key (i.e. back up key) if the first public key is not valid. The examiner respectfully disagrees, Sudia discloses multiple instruction keys of the trusted third parties in the device firmware besides manufacturer's signature key, if the manufacturer's key is compromised, lost or destroyed (i.e. key is not valid), then the trusted third party's instruction key can be used

to replace, as such the replacement key is viewed as the second key or backup key to efficiently provide a recovery system (Sudia: paragraph 0251).

### ***Claim Objections***

4. The objections of claims 1, 27 and 32 have been withdrawn based on the filed amendments.

### ***Claim Rejections - 35 USC § 112***

5. The rejections under 35 U.S.C. 112, first paragraph have been withdrawn based on the filed amendments.

### ***Claim Rejections - 35 USC § 102***

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 33-35 and 38-41 are rejected under 35 U.S.C. 102(e) as being anticipated by Hind et al. (6,976,163).

a) As to claim 33, Hind discloses a method comprising storing a first portion of a firmware code which is not upgradable in a first reprogrammable semiconductor memory (i.e. permanent and non-modifiable content is stored in read only memory 240,

Hind: col. 8, lines 41-44); providing a second portion of a firmware code that is upgradable in said first reprogrammable semiconductor memory (i.e. semi-permanent and modifiable are in the programmable memory 236, Hind: col. 8, lines 37-41); and providing information for authenticating an upgrade of the second portion in the first portion (Hind: col. 3, lines 47-49; col. 8, lines 57-60). Hind further discloses a single memory array may be utilized to provide the programmable memory, the read only memory and the system memory (Hind: col. 9, lines 30-33), as such the first portion and second portion of a firmware code can be in a single memory.

b) As to claim 34, Hind discloses locking the first portion to prevent reading said first portion (i.e. preventing read operations to the ROM, Hind: col. 7, lines 35-53).

c) As to claims 35 and 38, Hind discloses providing a signature authentication in said first portion and providing instructions in said first portion to confirm the validity of a firmware upgrade file (Hind: col. 8, lines 57-60; col. 10, lines 54-67).

d) As to claim 39, Hind discloses determining whether an upgrade request is authentic and if said upgrade request is not authentic, locking the second portion against being written (Hind: col. 12, lines 45-55).

e) As to claim 40, this claim is directed to a hardware implementation of the method of claim 33 and is rejected by a similar rationale applied against claim 33.

f) As to claim 41, Hind discloses a public key is included in said second portion (Hind: col. 12, lines 22-32).

***Claim Rejections - 35 USC § 103***

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. Claims 1, 3, 5-7, 27 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Angelo et al. (5,748,940) in view of Falik et al. (2002/0166061) and further in view of Sudia (2001/0050990).

a) As to claims 1 and 27, Angelo discloses a secure updating of non-volatile memory comprising identifying a firmware upgrade request by a firmware program (i.e. a flash bit set to indicate a flash update will occur, Angelo: col. 3, lines 3-6); retrieving a file signed with a private key (Angelo: Fig. 3, element 310); validating a file with a public key (Angelo: Fig. 3, element 312; col. 3, lines 39-52); upgrading a portion of the firmware program (Angelo: Fig. 3, element 316).

Angelo does not disclose locking a device storing the firmware program such that a second portion of the firmware program is not readable.

Falik discloses an apparatus and method for protecting the contents of a shared memory in a memory device comprising a step of locking a device storing the firmware program such that a second portion of the firmware program is not readable (Falik: page 2, paragraph [0015]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of locking device storing the firmware program such that a

second portion of the firmware program is not readable in the system of Angelo, as Falik teaches, so as to prevent access to the firmware by unauthorized users.

Angelo and Falik do not disclose the steps of validating the public key and retrieving a second public key from the firmware program if the public key is not valid.

Sudia discloses a cryptographic system and method for upgrading device firmware (Abstract) of a trusted device comprising validating the public key and retrieving a second public key from the firmware program if the public key is not valid (Sudia: page 22, paragraph [0251]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of validating the public key and retrieving a second public key from the firmware program if the public key is not valid in the system of Angelo and Falik as Sudia teaches so as to efficiently perform firmware upgrade request.

b) As to claim 3, the combination of Angelo, Falik and Sudia discloses identifying a firmware upgrade request by a firmware program further comprising reading a flag, wherein the flag is located in a non-volatile medium (Angelo: Fig. 1, element 120; i.e. flash bit) and determining that the flag is set (Angelo: col. 2, lines 6-8).

c) As to claims 5 and 29, the combination of Angelo, Falik and Sudia discloses locking flags is utilized to implement software protection for each flash memory device blocks (Falik: page 1, paragraph [0014]; i.e. determining that the file is not authentic and locking the device).

d) As to claim 6, the combination of Angelo, Falik and Sudia discloses locking the device after upgrading a portion of the firmware program by the firmware program (Falik: page 9, paragraph [0111]; page 11, paragraph [0122]).

e) As to claim 7, the combination of Angelo, Falik and Sudia discloses the second portion of the firmware program is a public key (Angelo: col. 3, lines 39-52).

10. Claims 4 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Angelo et al. (5,748,940) in view of Falik et al. (2002/0166061) in view of Sudia (2001/0050990) and further in view of Toft (2002/0138592).

a) As to claim 32, Angelo discloses a secure updating of non-volatile memory comprising identifying a firmware upgrade request by a firmware program (i.e. a flash bit set to indicate a flash update will occur, Angelo: col. 3, lines 3-6); retrieving a file signed with a private key (Angelo: Fig. 3, element 310); validating a file with a public key (Angelo: Fig. 3, element 312; col. 3, lines 39-52); upgrading a portion of the firmware program (Angelo: Fig. 3, element 316).

Angelo discloses identifying a firmware upgrade request by a firmware program further comprising reading a flag, wherein the flag is located in a non-volatile medium (Angelo: Fig. 1, element 120; i.e. flash bit) and determining that the flag is set (Angelo: col. 2, lines 6-8).

Angelo does not disclose locking a device storing the firmware program such that a second portion of the firmware program is not readable.



Falik discloses an apparatus and method for protecting the contents of a shared memory in a memory device comprising a step of locking a device storing the firmware program such that a second portion of the firmware program is not readable (Falik: page 2, paragraph [0015]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of locking device storing the firmware program such that a second portion of the firmware program is not readable in the system of Angelo as Falik teaches so as to prevent access to the firmware by unauthorized users.

Angelo and Falik do not disclose the steps of validating the public key and retrieving a second public key from the firmware program if the public key is not valid.

Sudia discloses a cryptographic system and method for upgrading device firmware (Abstract) of a trusted device comprising validating the public key and retrieving a second public key from the firmware program if the public key is not valid (Sudia: page 22, paragraph [0251]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of validating the public key and retrieving a second public key from the firmware program if the public key is not valid in the system of Angelo and Falik as Sudia teaches so as to efficiently perform firmware upgrade request.

Angelo, Falik and Sudia do not explicitly disclose the steps of deleting the file and clearing the flag.

Toft discloses clearing the update flag before rebooting the system (Toft: paragraph [0022]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of clearing the update flag in the system of Angelo, Falik and Sudia as Toft teaches so as to properly control the update process.

Angelo, Falik, Sudia and Toft do not explicitly disclose deleting the file.

The examiner takes official notice that deleting the upgrade file after it is being used is a common practice to save system memory.

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of deleting the file in the system of Angelo, Falik, Sudia and Toft so as to save system memory.

b) As to claim 4, please see addressed above claim 32.

11. Claims 36-37 and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hind et al. (6,976,163) in view of Sudia (2001/0050990).

Hind discloses a public key is provided in the second portion (Hind: col. 12, lines 22-32), however Hind is silent on the capability of having two public keys (claims 36 and 42) and two identical public keys (claim 37).

Sudia is relied on for the teaching of having two public keys and they are identical (Sudia: paragraphs [0251]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having two public keys and two identical public keys in the system of Hind as Sudia teaches so as to provide a back up key in the case the other key is lost or stolen (i.e. not valid).

***Conclusion***

**12. THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MinhDieu Nguyen whose telephone number is 571-272-3873.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Application/Control Number:  
09/922,041  
Art Unit: 2137

Page 11

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



MinhDieu Nguyen  
Patent Examiner  
Art Unit 2137  
11/12/07